* 1. **SKOP**

Dasar ini terpakai kepada semua projek pembangunan perisian dan sistem yang dijalankan dalam organisasi, termasuk alat dalaman, sistem pihak ketiga *(third-party system)*, pembangunan luar, dan *cloud-based applications*. Ia terpakai kepada semua pekerja, kontraktor, dan pihak ketiga yang terlibat dalam pembangunan dan aktiviti kitaran hidup sistem. Semua kod mesti mematuhi prinsip yang digariskan dalam Polisi Kod Selamat *(Code Review/Secure Coding Policy)* dan Pelan Pemulihan Bencana, Sandaran dan Keterlangsungan Perniagaan *(Disaster Recovery Plan, Backup and Business Continuity).*

1. **TANGGUNGJAWAB**

Sasaran utama untuk dasar ini termasuk pentadbir IT, pegawai keselamatan, pembangunan sistem, dan kakitangan yang terlibat dalam keselamatan sistem atau rangkaian. Ia juga terpakai kepada pasukan audit dalaman dan pihak pengurusan yang bertanggungjawab untuk perlindungan data dan mitigasi risiko.

|  |  |
| --- | --- |
| **Peranan** | **Tanggungjawab** |
| Pembangun Sistem | Melaksanakan kod yang selamat dan mengikut garis panduan SSDLC |
| Pasukan Keselamatan | Menilai kawalan keselamatan |
| Menjalankan penilaian risiko dan ujian keselamatan |
| Pengurus Projek | Memastikan semua peringkat SSDLC dipatuhi dan didokumentasikan |
| Operasi IT | Menguruskan pelaksanaan sistem dan tugas penyelenggaraan dengan selamat. |
| Audit Dalaman | Memantau pematuhan terhadap dasar ini dan amalan terbaik SSDLC |

1. **DOKUMEN RUJUKAN**

|  |  |
| --- | --- |
| **Kod Dokumen** | **Tajuk Dokumen** |
|  | Code Review/Secure Coding Policy |
|  | Disaster Recovery, Backup, and Business Continuity Plan |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

1. **TERMINOLOGI DAN SINGKATAN**

|  |  |  |
| --- | --- | --- |
| PTPKM | : | Pusat Teknologi dan Pengurusan Kriptologi Malaysia |
| KS | : | Ketua Seksyen yang bertugas di Seksyen iDEC yang  dipertanggungjawabkan |
| Pembekal | : | Pembekal sah yang dilantik oleh iDEC untuk kerja-kerja perkhidmatan dan penyelenggaraan |
| PYB | : | Pekerja Yang Bertanggungjawab |
| Pekerja ICT | : | Pegawai Teknologi Maklumat/Jurutera/Penolong Pegawai  Teknologi Maklumat/Penolong Jurutera/Juruteknik Komputer/Pekerja lain yang dilantik untuk mengurus ICT |
| Pentadbir Sistem | : | Pegawai Teknologi Maklumat/Jurutera/Penolong Pegawai Teknologi Maklumat/Penolong Jurutera/Juruteknik Komputer/Pekerja lain yang mengurus operasi atau aktiviti berkaitan  pengoperasian aplikasi, telekomunikasi serta pengurusan sistem pangkalan data Universiti. |
| TPKD | : | Timbalan Pegawai Kawalan Dokumen |
| TWP | : | Timbalan Wakil Pengurusan |
| WP | : | Wakil Pengurusan |
| SSDLC | : | *Secure Software Life Cycle* |
| UAT | : | *User Acceptance Testing* |
| PDPA | : | *Personal Data Protection Act* |
| NIST | : | *National Insitute of Standards and Technology* |
| ISO/IEC | : | *International Organization for Standardization/International Electrotechnical Commission* |
| COTS | : | *Commercial Off-The-Shelf* |
| RBAC | : | *Role-Based Access Control* |
| OWASP | : | *Open Worldwide Application Security Project* |
| ITIL | : | *Information Technology Infrastructure Library* |
| SDLC | : | *Software Development Life Cycle* |

1. **KENYATAAN DASAR *(Policy Statements)***
   1. **Pembangunan Sistem *(System Development)***
      * Semua pembangunan sistem mesti mengikuti rangka kerja SSDLC seperti yang digariskan dalam panduan negara seperti Panduan SSDLC CyberSecurity Malaysia.
      * Aktiviti projek pembangunan sistem mesti merangkumi perkara berikut:
        + Permulaan/Definisi Projek *(Project Initiation/Definition)*
        + Penilaian Risiko *(Risk Assessment)*
        + Pengenalpastian Keperluan Pengguna (Fungsi dan Bukan Fungsi) *(Identification of Functional and Non-functional User Requirements)*
        + Reka Bentuk Sistem *(Systems Design)*
        + Pembangunan Sistem *(System Development)*
        + Jaminan Kualiti *(Quality Assurance)*
        + Dokumentasi dan Latihan *(Documentation and Training)*
        + Ujian dan Penerimaan Sistem *(Systems Testing and Acceptance)*
        + Pelaksanaan *(Deployment)*
        + Penyelenggaraan *(Maintenance)*
      * Semua sistem *COTS* dan aplikasi *custom* mesti melaksanakan kawalan akses berasaskan peranan *(RBAC).* Pentadbir akses mesti menguruskan hak akses dan jika mereka juga pengguna, mereka perlu mempunyai akaun yang berasingan bagi akses pentadbiran dan akses pengguna.
      * Kawalan keselamatan mesti diterapkan pada setiap peringkat pembangunan, bermula dari fasa perancangan *(planning)* hingga ke pelaksanaan *(deployment)*.
      * Kod sumber *(source code)* mesti dikawal versi *(version-controlled)* dan disimpan dengan selamat di dalam repositoriyang mematuhi Polisi Kod Selamat *(Secure Coding Policy)* bagi mengelakkan akses dan pengubahsuaian tanpa kebenaran.
      * Semua komponen/perpustakaan pihak ketiga *(third-party libraries)* mesti dinilai untuk kerentanan *(vulnerabilities)* sebelum diintegrasikan.
      * Persekitaran pengeluaran *(production)*, pembangunan *(development)*, dan ujian *(testing)* mesti dipisahkan secara logik. Semua ujian di persekitaran pengeluaran mesti menggunakan data yang telah dinyahidentifikasi *(sanitized).*
   2. **Ujian Sistem *(System Testing)***
      * Semua sistem mesti menjalankan beberapa peringkat ujian, termasuk:
        + Ujian Unit
        + Ujian Integrasi
        + Ujian Sistem
        + Ujian Penerimaan Pengguna *(UAT)*
        + Ujian Keselamatan (termasuk analisis statik/dinamik dan penilaian kerentanan *(vulnerability assessment)*).
      * Ujian hendaklah dijalankan dalam persekitaran yang terasing dan terkawal dan mencerminkan keadaan pengeluaran sebenar, tetapi tidak melibatkan data sebenar atau sensitif.
      * Laluan akses aplikasi bukan produksi *(Non-production application access paths)* mesti dipadam atau dinyahaktifkan.
      * *Debugging code,* ID pengguna ujian dan kata laluan mesti dikeluarkan sebelum pelancaran selaras dengan Garis Panduan Penyebaran Selamat *(Secure Deployment Guidelines)* OWASP dan NIST SP XXXX-XXX.
      * Semua kod sebelum pelancaran mesti disemak oleh individu selain penulis asal dan oleh mereka yang mahir dalam teknik dan amalan semakan kod, seperti yang digariskan dalam Polisi Semakan Kod/Kod Selamat.
      * Semakan kod dan ujian kes penggunaan mesti dilakukan oleh pegawai dalaman yang layak atau pihak ketiga yang dilantik seperti dinyatakan dalam Polisi Semakan Kod/Kod Selamat.
      * Ujian mesti didokumentasikan, boleh diulang dan dilaksanakan dalam persekitaran yang terkawal.
      * Log ujian mesti disimpan dengan selamat dan hanya boleh diakses oleh pihak yang dibenarkan.
      * Sebarang kerentanan *(vulnerabilities)* yang dikenal pasti mesti diselesaikan sebelum pelaksanaan kepada produksi *(production deployment)*.
      * Ujian penembusan *(penetration testing)* mesti dijalankan sebelum pelancaran rasmi.
      * Kakitangan pembangunan dan sistem mesti mengikut jadual pelancaran yang diluluskan oleh pentadbir.
   3. **Penyelenggaraan Sistem *(System Maintenance)***
      * *Patching* dan kemas kini yang berkala mesti dijadualkan untuk menangani kerentanan keselamatan *(security vulnerabilities)* dan penambahbaikan sistem.
      * Penyelenggaran sistem hendaklah mematuhi Proses Pengurusan Perubahan *(Change Management Process)* yang formal berdasarkan amalan terbaik ITIL dan standard ISO/IEC XXXXX.
      * Prosedur pengurusan perubahan mesti diikuti untuk semua kemas kini dan penambahbaikan.
      * Akses kha yang digunakan semasa penyelenggaran hendaklah dikawal rapi, dihadkan tempohnya *(time-bound)*, dan diaudit selaras dengan standard ISO/IEC XXXXX.
      * Aktiviti penyelenggaraan mesti dipantau dan direkodkan, serta hanya dibenarkan oleh kakitangan yang dilantik.
      * Pelan pengunduran *(rollback)* mesti disediakan sekiranya berlaku risiko atau kegagalan baru selepas penyelenggaraan, selaras dengan Pelan Pemulihan Bencana, Sandaran dan Keterlangsungan Perniagaan *(Disaster Recovery, Backup and Business Continuity Plan).*
      * Sistem mesti dipantau selepas penyelenggaraan untuk mengenal pasti sebarang aktiviti atau isu prestasi *(performance)* yangtidak normal.
      * Sistem lama *(legacy)* mesti dinilai secara berkala dari sudut pematuhan terhadap keperluan keselamatan dan tahap sokongan teknikal *(supportability)*. Sistem yang tidak lagi diperlukan mesti dinyahaktifkan dengan selamat.
   4. **Dokumentasi *(Documentation)***
      * Semua fasa SDLC mesti didokumentasikan dan disimpan dengan selamat.
      * Keputusan penting, kelulusan, dan perubahan mesti boleh dijejaki untuk tujuan audit dan pematuhan.
2. **PEMATUHAN DAN PEMANTAUAN**
   1. **Audit Berkala**

Audit dalaman akan dijalankan secara berkala untuk memastikan pematuhan terhadap proses SSDLC dan piawaian yang berkenaan seperti PDPA, NIST, dan ISO/IEC XXXXX. Audit ini akan memfokuskan pada amalan pembangunan, ujian dan penyelenggaran sistem.

Kegagalan untuk mematuhi akan mengakibatkan tindakan pembetulan yang mungkin melibatkan tindakan disiplin. Semua aktiviti yang berkaitan dengan pembangunan, ujian, dan penyelenggaran mesti mematuhi dasar keselamatan organisasi, termasuk kawalan akses, perlindungan data, dan piawaian pengekodan yang selamat. Penilaian keselamatan yang berkala, termasuk imbasan kerentanan *(vulnerabilty scanning)* dan penilaian risiko, juga akan dijalankan secara berkala.

* 1. **Latihan**

Semua kakitangan yang terlibat dalam pembangunan, ujian atau penyelenggaraan mesti menerima latihan berkala mengenai amalan pengekodan yang selamat, prinisip SSDLC dan keperluan pematuhan yang berkaitan .

1. **SEMAKAN DAN KEMASKINI DASAR**

Dasar ini akan disemak semula setiap tahun atau apabila perubahan besar berlaku dalam teknologi, peraturan, atau sistem dalaman. Pasukan Keselamatan Maklumat akan mengemukakan cadangan kemaskini, yang mesti diluluskan dan dikomunikasikan kepada semua pasukan yang terlibat.

1. **LAMPIRAN**